Division of Information Technology Services
Department of Administrative Services
State of Utah

November 2, 2000

Robert D. Woolley
State Technical Architect

Enterprise Security Policy Development Methodology

Introduction

The State has made a number of attempts to develop a State Information Security policy over the last several years, and some useful work has been completed that will result in a potentially useful set of security policies and procedures. As security teams become more effectively organized at enterprise and agency levels, and as the State expands its presence on the Internet, the need for an actionable set of security policies has become evident. Policy adherence among Global 2000 organizations is generally low "with only 25% of organizations claiming to be 'almost always' compliant." Reasons for low levels of compliance have included "lack of executive buy-in, no visible management support, and immature, expensive enforcement technology." These problems are only worsened by inconsistent and uncoordinated policy development with agencies.

The types of policies needed are largely dictated by the nature and deployment of the technical infrastructure within the State. From a business impact perspective the META Group has suggested that:

> "Successful IT-enabled business processes depend on effective information security, which is predicated on effective policies. Security weaknesses expose the business to potential embarrassment, financial loss, and even ruin."

A consistent approach to policy definition, documentation, and enforcement are important to improve policy adherence and ultimately to afford meaningful protection to State technology resources.

Types of Policies

Security policies can be classified into three basic groups, each of which are important to the State:

- ***State Information Security Charter:*** This document sets the overall tone for information security within the organization. The charter must be clearly endorsed by executive management. This document identifies the need for security; defines the scope of the policy; identifies responsibility for major security functions within the enterprise; defines the scope of contingency and disaster recovery in the event of a security breach; and specifies any legal, regulatory or audit requirements that have to be met. This document is signed by the Governor and supported by the Cabinet.

- ***State Information Security Policy:*** This is the information security policy that applies to the overall infrastructure of the organization and all persons that use it. (For example: unique user ID and password combinations will govern all access to IT network resources.) The generic policy for the enterprise is the building block upon which agency and specific information security policies can be developed. This policy document is intended to be reasonably short and suitable for employees to read and sign a compliance agreement with the provisions of the policy.

- ***Specific Policies:*** These policies apply to specific infrastructure domains:
  - ❑ *Resource Based Polices:* These policies prescribe access and rights from the perspective of specific resources such as, files, applications, and networks.
  - ❑ *Person Based Policies:* These policies prescribe access and rights from an individual perspective. A specific user A can access resources X, Y, and Z.
  - ❑ *Role Based Policies:* These policies provide abstraction between persons and resources. For example all persons who are agency directors or equivalent can access payroll information on payroll servers and approve payroll hours. These policies simplify the management of people to resources.
  - ❑ *Configuration Policies:* These policies govern the infrastructure configuration rules, such as the nature and structure of passwords, or operating system configuration settings.
  - ❑ *Behavioral Policies:* These policies guide the day-to-day behavior of employees regarding information security such as acceptable use, release of confidential information to third parties, password control issues, etc. These policies are generally enforced with regular auditing and organizational sanctions.

The relationship of each of these policy types is illustrated in Figure 1.

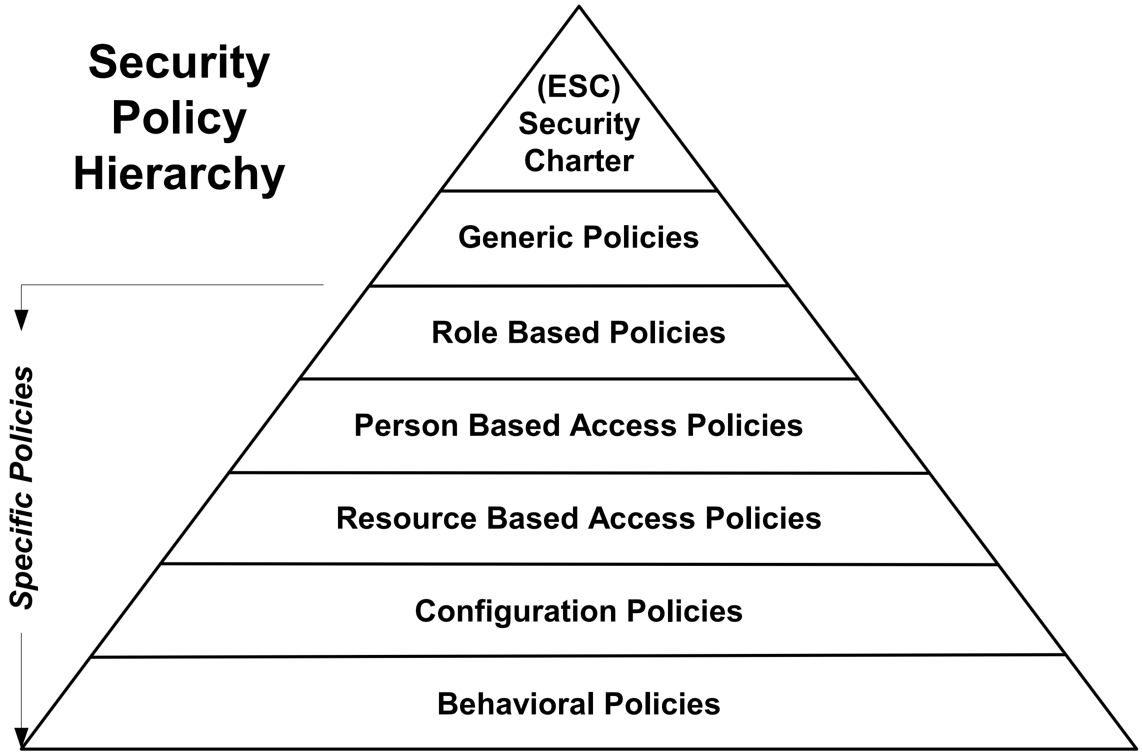

Figure 1. Security Policy Hierarchy

Implementation
Security policy implementation for the State of Utah suggests the need for the following steps and associated timelines:

▪ November 13, 2000	The State Information Security Committee (SISC) will review the draft State Information Security Charter and the draft State Information Security Policy.
▪ January 8, 2001	SISC approval of the State Information Security Policy and State Information Security Charter for the state. Referral to the ITPSC for discussion and approval in the January 2001 meeting
▪ February 2001	SISC approval of State Firewall and Network Access Policies. Identify other security policies that require development.
▪ March 2001	Complete drafts of other identified enterprise policies dealing with resources, persons, roles, configuration, and behaviors, and present the policies for preliminary comment to SISC in the March 2001 meeting.
▪ March 2001	Approval of Firewall and Network Access policies in the March ITPSC Meeting.
▪ April 2001	Review and update other identified security policy drafts.
▪ May 2001	SISC vote on other security policy drafts.
▪ May 2001	Present other security policy drafts to the ITPSC for comment and/or approval.

Note: Copies of all security policy documents are routinely distributed for comment to SISC and related State security groups, IT Managers/Directors of agencies, the CIO, and relevant ITS staff.